

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problems Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-312680

(43)Date of publication of application : 09.11.2001

(51)Int.Cl. G06F 17/60

(21)Application number : 2001-122699

(71)Applicant : LUCENT TECHNOL INC

(22)Date of filing : 20.04.2001

(72)Inventor : JAKOBSSON BJORN M
REITER MICHAEL KENDRICK
SILBERSCHATZ ABRAHAM

(30)Priority

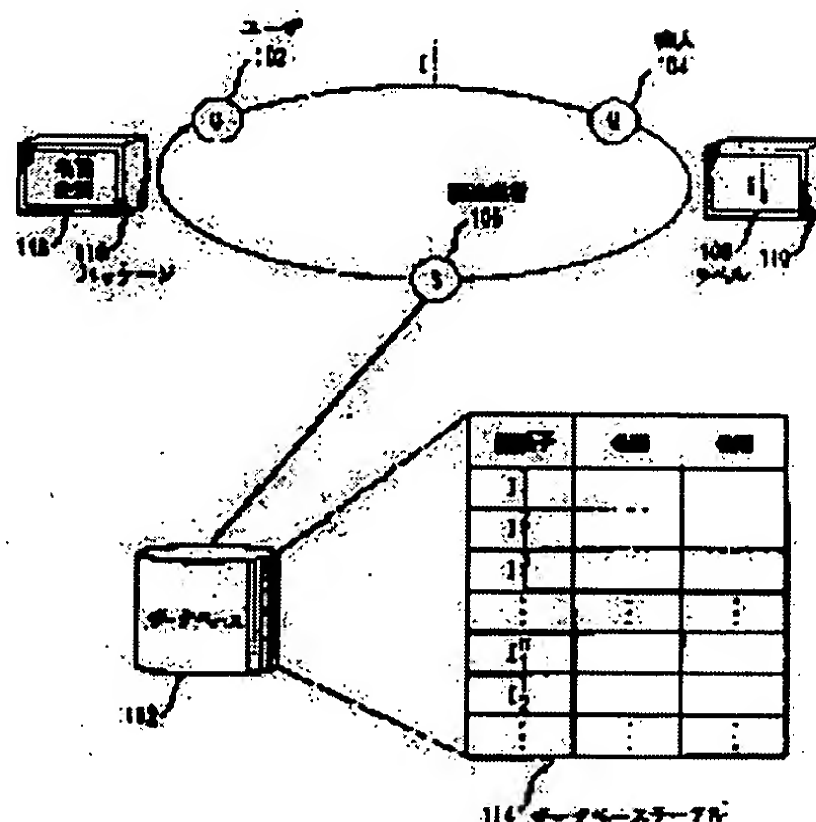
Priority number : 2000 561535 Priority date : 28.04.2000 Priority country : US

(54) METHOD FOR ELECTRONIC COMMERCE AND DATA BASE

(57)Abstract:

PROBLEM TO BE SOLVED: To provide an anonymous delivery method which cannot be linked in electronic commerce.

SOLUTION: The anonymous delivery/payment method used in connection with electronic commerce is provided. A user starts electronic transaction with a merchant and therefore a specific identifier is supplied to the merchant. For starting respective transactions by the user, the specific identifier supplied to various traders is changed. The merchant attaches the identifier to a label on a package including the commodity which is to be delivered to the user by the reception of the identifier and the package is supplied to the delivery agent being a third person to whom the package is entrusted. The delivery agent accesses a data base for relating the identifier to the address of the specified user. The delivery agent exchanges the label for the label including the name and the address of the user and delivers the package to the user.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the
examiner's decision of rejection or application
converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of
rejection][Date of requesting appeal against examiner's decision
of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(19)日本国特許庁 (J P)

(12) 公 開 特 許 公 報 (A)

(11)特許出願公開番号

特開2001-312680

(P2001-312680A)

(43)公開日 平成13年11月9日(2001.11.9)

| | | | |
|--------------------------|-------|---------------|-------------|
| (51)Int.Cl. ⁷ | 識別記号 | F I | ターマコード*(参考) |
| G 0 6 F 17/60 | 4 2 4 | G 0 6 F 17/60 | 4 2 4 |
| | 3 1 0 | | 3 1 0 E |
| | 3 3 4 | | 3 3 4 |
| | 4 3 0 | | 4 3 0 |
| | Z E C | | Z E C |

審査請求 未請求 請求項の数40 O L (全 14 頁)

(21)出願番号 特願2001-122699(P2001-122699)

(22)出願日 平成13年4月20日(2001.4.20)

(31)優先権主張番号 09/561535

(32)優先日 平成12年4月28日(2000.4.28)

(33)優先権主張国 米国 (U S)

(71)出願人 596077259
ルーセント テクノロジーズ インコーポ
レイテッド
Lucent Technologies
Inc.
アメリカ合衆国 07974 ニュージャージ
ー、マレーヒル、マウンテン アベニュー
600-700

(74)代理人 100081053
弁理士 三俣 弘文

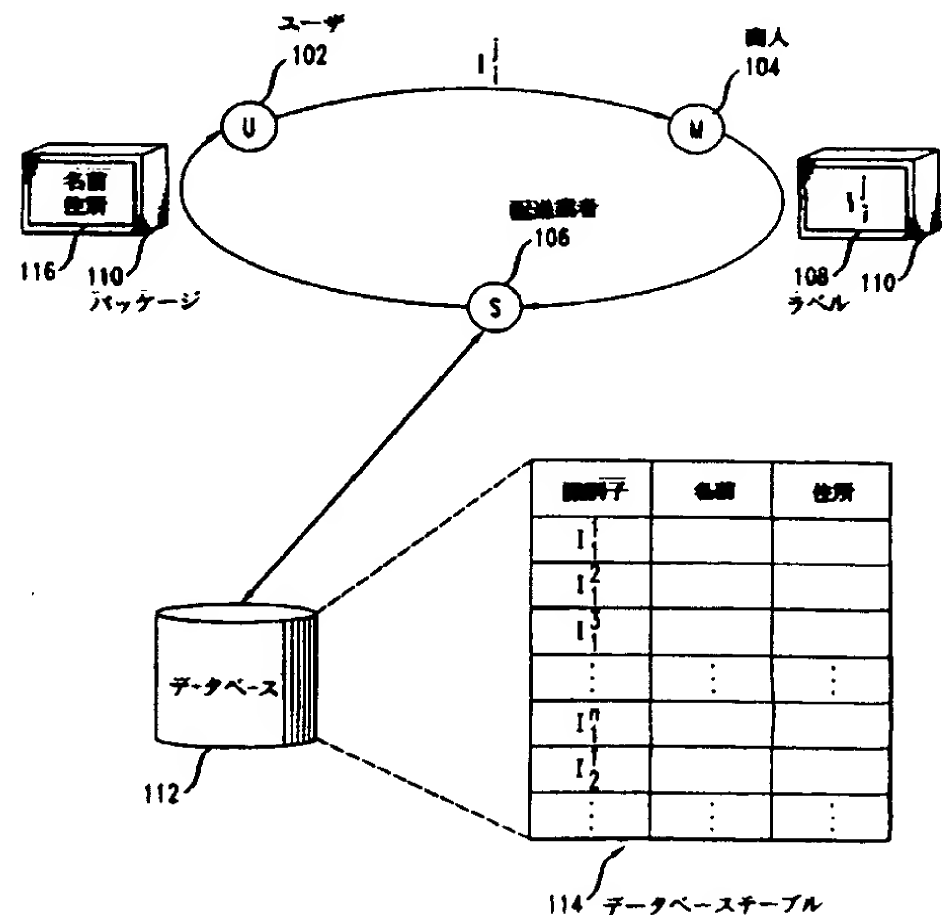
最終頁に続く

(54)【発明の名称】 電子商取引のための方法およびシステムおよびデータベース

(57)【要約】

【課題】 エレクトロニックコマースにおけるリンク可
能でない匿名性配達技法を提供すること。

【解決手段】 エレクトロニックコマースとの関連で使
用するための匿名の配達および支払い技法である。ユー
ザは、商人との電子的取引に入ることにより、固有の識
別子を商人に提供する。このユーザにより各取引に入る
ために、様々な商人に提供される固有の識別子は変化す
る。識別子の受け取りにより、商人は、その識別子をユ
ーザに配達されるべき商品を含むパッケージ上のラベル
に付け、このパッケージを委託された第三者の配送業者
に提供する。配送業者は、識別子を特定のユーザの住所
に関連づけるために、データベースにアクセスする。そ
の後、配送業者は、そのラベルを、ユーザの名前および
住所を含むラベルと取り替え、そのパッケージをユーザ
に配達する。



【特許請求の範囲】

【請求項1】 商人から識別子を受け取るステップと、
前記受け取られた識別子に基づいて複数のユーザのうちの1つを同定するステップと、

前記一人のユーザの住所を決定するステップとを有し、
前記複数のユーザの各々は、少なくとも2つの異なる受け取られた識別子に基づいて、同定され得ることを特徴とする方法。

【請求項2】 パッケージを前記決定されたアドレスにおける前記一人のユーザに配送するステップをさらに含むことを特徴とする請求項1記載の方法。

【請求項3】 前記同定するステップは、
前記受け取られた識別子を使用してデータベースルックアップを実行するステップを含むことを特徴とする請求項1記載の方法。

【請求項4】 前記データベースルックアップで、前記一人のユーザを同定することができなかった場合、
少なくとも1つの識別子を生成し、
前記生成された識別子を前記受け取られた識別子と比較するステップをさらに含むことを特徴とする請求項3記載の方法。

【請求項5】 前記少なくとも1つの識別子を生成するステップは、
前記データベースに記憶された情報を使用して前記少なくとも1つの識別子を生成するステップを含むことを特徴とする請求項4記載の方法。

【請求項6】 前記少なくとも1つの識別子を生成するステップは、
前記商人から受け取られた追加的情報を使用して、前記少なくとも1つの識別子を生成するステップを含むことを特徴とする請求項5記載の方法。

【請求項7】 前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項6記載の方法。

【請求項8】 前記カウンターは暗号化されていることを特徴とする請求項7記載の方法。

【請求項9】 前記識別子は、前記商人からパッケージラベル上で受け取られることを特徴とする請求項1記載の方法。

【請求項10】 前記受け取られた識別子は、記憶された値の第1の部分であり、前記方法は、
前記商人からメッセージおよび第1の暗号化されたメッセージを受け取るステップと、
前記記憶された値の第2の部分を検索するステップと、
第2の暗号化されたメッセージを生成するために、前記値の前記第2の部分を使用して前記受け取られたメッセージを暗号化するステップと、
前記第1の暗号化されたメッセージが、第2の暗号化されたメッセージと一致するかどうかを決定するステップをさらに含むことを特徴とする請求項1記載の方法。

【請求項11】 前記第1の暗号化されたメッセージが、前記第2の暗号化されたメッセージと一致する場合、前記受け取られたメッセージを有効化するステップをさらに含むことを特徴とする請求項10記載の方法。

【請求項12】 前記メッセージは、金額を示すことを特徴とする請求項11記載の方法。

【請求項13】 前記同定するステップは、
前記データベースに記憶された情報を使用して少なくとも1つの識別子を生成するステップを含むことを特徴とする請求項1記載の方法。

【請求項14】 前記少なくとも1つの識別子を生成するステップは、
前記商人から受け取られた追加的情報を使用して、前記少なくとも1つの識別子を生成するステップを含むことを特徴とする請求項13記載の方法。

【請求項15】 前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項14記載の方法。

【請求項16】 前記商人から受け取られた前記追加的情報は、ランダム数を含むことを特徴とする請求項14記載の方法。

【請求項17】 商人から受け取られた識別子を読み取るための手段と、前記受け取られた識別子に基づいて複数のユーザのうちの一人を同定するための手段と、
前記一人のユーザの住所を決定するための手段とを有し、
前記複数のユーザの各々は、少なくとも2つの異なる受け取られた識別子に基づいて同定され得ることを特徴とするシステム。

【請求項18】 前記識別子を読み取るための手段は、
バーコードスキャナであることを特徴とする請求項17記載のシステム。

【請求項19】 前記同定するための手段は、
前記受け取られた識別子を使用してデータベースルックアップを実行するための手段を含むことを特徴とする請求項17記載のシステム。

【請求項20】 前記データベースルックアップが失敗した場合に使用するために、
少なくとも1つの識別子を生成するための手段と、
前記受け取られた識別子と前記生成された識別子と比較するための手段とをさらに含むことを特徴とする請求項19記載のシステム。

【請求項21】 前記少なくとも1つの識別子を生成するための手段は、
前記データベース中に記憶された情報を使用して前記少なくとも1つの識別子を生成するための手段を含むことを特徴とする請求項20記載のシステム。

【請求項22】 前記少なくとも1つの識別子を生成するための手段は、
前記商人から受け取られた追加的情報を使用して前記少

なくとも1つの識別子を生成するための手段をさらに含むことを特徴とする請求項21記載のシステム。

【請求項23】 前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項22記載のシステム。

【請求項24】 前記カウンターは暗号化されていることを特徴とする請求項23記載のシステム。

【請求項25】 前記識別子は、前記商人から、パッケージラベル上で受け取られることを特徴とする請求項17記載のシステム。

【請求項26】 前記受け取られた識別子は、記憶された値の第1の部分であり、前記システムは、前記商人からメッセージおよび第1の暗号化されたメッセージを受け取るための手段と、前記記憶された値の第2の部分を検索するための手段と、第2の暗号化されたメッセージを生成するために、前記値の前記第2の部分を使用して、前記受け取られたメッセージを暗号化するための手段と、前記第1の暗号化されたメッセージが、前記第2の暗号化されたメッセージと一致するかどうかを決定するための手段とをさらに含むことを特徴とする請求項17記載のシステム。

【請求項27】 前記第1の暗号化されたメッセージが、前記第2の暗号化されたメッセージに一致する場合、前記受け取られたメッセージを有効化するための手段をさらに含むことを特徴とする請求項26記載のシステム。

【請求項28】 前記メッセージが、金額を示すことを特徴とする請求項27記載のシステム。

【請求項29】 前記同定するための手段は、前記データベース中に記憶された情報を使用して、少なくとも1つの識別子を生成するための手段を含むことを特徴とする請求項17記載のシステム。

【請求項30】 前記少なくとも1つの識別子を生成するための手段は、

前記商人から受け取られた追加的情報を使用して、前記少なくとも1つの識別子を生成するための手段を含むことを特徴とする請求項29記載のシステム。

【請求項31】 前記商人から受け取られた前記追加的情報は、カウンターを含むことを特徴とする請求項30記載のシステム。

【請求項32】 前記商人から受け取られた前記追加的情報は、ランダム数を含むことを特徴とする請求項30記載のシステム。

【請求項33】 受け取られた識別子を住所と関連づけるために配送業者により使用するためのデータベースであって、各々がデータを記憶するための複数のフィールドを含む複数の記録を含み、前記記録の各々が、少なくとも、1つの固有の識別子および1つの住所を記憶し、

少なくとも2つの記録が、異なる固有の識別子および同じ住所を含むことを特徴とするデータベース。

【請求項34】 前記記録の各々が、少なくとも、1つのカウンターおよび1つのキーを記憶し、前記固有の識別子は、前記カウンターおよび前記キーの関数であることを特徴とする請求項33記載のデータベース。

【請求項35】 前記固有の識別子は、第1の部分および第2の部分を含むことを特徴とする請求項33記載のデータベース。

【請求項36】 受け取られた識別子と住所とを関連づけるために、配送業者により使用するためのデータベースであって、各々が、データを記憶するための複数のフィールドを含む複数の記録を含み、前記記録の各々は、少なくとも、

1つの固有の識別子、

1つのカウンター、

1つのキー、および

1つの住所を記憶し、

前記固有の識別子は、前記カウンターおよび前記キーの関数であることを特徴とするデータベース。

【請求項37】 特定のアドレスは、1つのデータベース記録中にのみあることを特徴とする請求項36記載のデータベース。

【請求項38】 受け取られた識別子が、前記データベース記録のうちの1つ中に記憶された固有の識別子と一致する場合、

前記1つのデータベース記録中の前記カウンターは、インクリメントされ、

前記1つのデータベース記録中の前記固有の識別子は、更新されることを特徴とする請求項37記載のデータベース。

【請求項39】 特定の住所は、少なくとも2つのデータベース記録中にあることを特徴とする請求項36記載のデータベース。

【請求項40】 前記識別子は、第1の部分および第2の部分を含むことを特徴とする請求項36記載のデータベース。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、エレクトロニックコマースに係り、特に、データネットワークを介して注文された商品の匿名のかつ安全な配達および支払いに関する。

【0002】

【従来の技術】電子商取引の数が増大しているので、プライバシーがますます重要になってきている。オンライン購入のトラッキングおよびプロファイリングの可能性のために、エレクトロニックコマースに関わることをためらう購入者がいる。そして、これらの購入者は、伝統

的な、特に現金の取引により提供される匿名性のために、従来の“brick and mortar”ビジネスを好む。

【0003】オンライン取引において匿名性を提供するための主要な障害は、オンラインで購入される商品が、購入者に物理的に配達されなければならないという電子的取引のまさに性質から生じる。勿論、これは、商品が配送され得るように、購入者が商人 (merchant) に彼の／彼女の名前および住所を提供することを必要とする。商人は、購入情報を集め、これを、マスメーリング (mass mailings) のようなマーケティング目的のために使用する。この匿名性の問題は、エレクトロニックコマース産業に対する主要な障害である。

【0004】1つの解決法は、米国特許第6, 006, 200 (“Boies et al.”) に示されており、ここでは、顧客の名前および住所情報が、配送業者のような信頼おける第三者のデータベースに預けられる。各顧客は、顧客の名前および住所に関連づけられたデータベース中に記憶された固有の識別子を受け取る。データベースエントリがセットアップされた後、顧客は、オンライン購入を行い、商人に固有の識別子のみを提供することができる。商人は、購入されたアイテムを含む物理的パッケージ上にその固有の識別子を付け、パッケージを委託された第三者の配送業者に提供する。そして、配送業者は、その固有の識別子に基づいて顧客の名前および住所を決定し、そのパッケージを顧客に配達する。

【0005】Boies 等による特許に示された技法は、あるレベルの匿名性を提供するが、この提案された解決法にはいくつもの問題がある。第1に、そのシステムにおける取引は、いわゆるリンク可能であり、一人または二人以上の商人は、購入情報がある期間について集めることができ、その集められた購入情報は、特定の識別子に関連づけられた購入者についての所定の情報が発見され得るように関連づけられ得る。期間が長く取引の回数が多い場合、特定の固有の識別子に関連づけられた購入者の名前および住所さえも、ある程度の正確さで決定され得る。

【0006】Boies 等による技法についての別の問題は、購入されたアイテムについての支払いを考慮に入れてないことである。配達メカニズムがある程度匿名であったとしても、購入に対する支払いは、別の問題および別の匿名性の欠如を提供する。ほとんどのオンライン購入は、クレジットカードを使用してなされるので、商人は、注文を処理するために、購入者の名前および住所を知らなければならない。勿論、Boies 等の特許において解決されていないが、匿名の支払いは、別の委託された第三者によりアレンジされ得る。しかし、そのような委託された第三者、購入者および商人の組合せを調整することは、ロジスティック的に困難である。

【0007】

【発明が解決しようとする課題】エレクトロニックコマ

ース産業を刺激するために必要とされているものは、リンク可能でない匿名性配達技法である。そのような配達技法が、購入者が匿名のままであることを可能にする改良された支払いスキームと組み合わせられ得る場合、更なる利益が得られる。

【0008】

【課題を解決するための手段】ユーザが商人から配送されるべき商品を購入するとき、ユーザは、商人に固有の識別子を提供する。その後、その商人は、商品を含むパッケージを、固有の識別子をユーザと関連づけることができる委託された第三者の配送業者に提供する。本発明によれば、そして従来技術と異なり、特定のユーザにより一人または二人以上の商人に提供される連続的な固有の識別子は、一連の取引の各々の間に変化する。

【0009】結果として、本発明の利点によれば、例えば長い期間について集められた多数の識別子の知識があっても、購入者およびその購入についてのいかなる有用な情報も提供しないことになる。各ユーザが複数の取引について同じ識別子を使用する従来技術による技法は、取引をリンク可能にしたが、複数の取引について異なる識別子を使用する本発明の技法は、取引をリンク不可能にする。

【0010】本発明の一実施形態によれば、商人は、ユーザから受け取った固有の識別子をパッケージラベルに付け、そのパッケージを第三者の委託された配送業者に提供し、その配送業者は、その固有の識別子をユーザと関連づけ、そのパッケージをユーザの住所に配達する。配送業者は、以前の登録プロセスの間に、既に複数の固有の識別子を特定のユーザに関連づけた。この事前の関連づけは、様々なやり方で行われ得る。

【0011】一実施形態において、配送業者は、複数の固有の識別子を生成し、これらの識別子をユーザに提供する。ユーザおよび配送業者の双方が、これらの識別子をコンピュータメモリ中に記憶する。その後、オンライン取引において、ユーザは、これらの識別子のうちの1つを商人に提供する。配送業者がラベル上に1つの識別子を有するパッケージを受け取るとき、配送業者は、受け取った識別子を見つけ、関連づけられたユーザの住所を決定するために、データベースルックアップを実行する。

【0012】別の実施形態によれば、ユーザおよび配送業者は、ユーザと配送業者との間で交換された既知のパラメータの値に基づいて、ダイナミックに識別子を生成することができる。特定の実施形態によれば、これらのパラメータは、連続的なオンライン取引の間、既知のインクリメントアルゴリズムによりインクリメントされるカウンターと共に、各ユーザに割り当てられた固有のキーである。各取引の後にカウンターは変化するので、連続的取引に関して商人により受け取られる識別子は、異なり、商人によりリンク不可能である。別の特定の実施

形態において、これらのパラメータは、ユーザにより生成されたランダム数を伴う固有のキーである。

【0013】以下にさらに詳細に説明する可能性のあるカウンター同期化エラーのために、配送業者は、各ユーザに対して、一連の固有の識別子を含む複数の記録を記憶することができる。これは、所定レベルの同期化エラーが存在したとしても、この技法が正しく動作することを可能にする。さらに別の技法によれば、同期化エラーが所定レベルを超えたとしても、ある識別子を適切なユーザと関連づけることは、外挿法の使用により実行され得る。新しい固有な識別子は、配送業者のデータベース情報のみを使用して、または配送業者に提供される追加の情報とも組合せで外挿され得る。

【0014】本発明の別の実施形態によれば、匿名の支払い技法は、上述した匿名の配達技法と組み合わされる。この実施形態によれば、配送業者は、商品について商人に支払い、ユーザは、商品について支払われた額、配送料、および任意的な取引処理料を配送業者に支払う。配送業者は、ユーザから商人に送られ、商人から配送業者に転送されたメッセージおよび暗号化されたメッセージを使用して、商品についての支払いに対するユーザの同意を認証する。

【0015】購入価格の認証により、配送業者は、ユーザが、配達される商品について特定の価格を支払うことを同意したことを確かに行うことができる。そして、配送業者は、商品について認証された額を商人に支払うことができ、配送業者は、ユーザがその商品について認証された額を支払うことを同意したことを確かに行うことができる。

【0016】

【発明の実施の形態】本発明の一実施形態を、図1を参照して説明する。図1は、ユーザU102、商人M104、および配送業者S106を含む。最初に、ユーザ102および商人104は、通信し、ユーザ102が商人104から商品を購入するという合意を合意する。この通信は、典型的には、データネットワーク（例えば、インターネット）を介して通信するユーザコンピュータと商人コンピュータによる。この時点において、我々は、商品についての支払いの問題を無視する。匿名の支払いを付け加える技法は、後述する。

【0017】販売の条件が合意されると、ユーザ102は、識別子 I_{ij} を商人104に送る。本発明の一側面によれば、そして従来技術と異なり、ユーザから商人に送られる識別子は、各取引で変化する。そして、 I_{ij} の表記は、 i 番目のユーザの j 番目の識別子を意味する。したがって、一連の取引の各々に対して、 i 番目のユーザは、一連の識別子 $I_{i1}, I_{i2}, I_{i3}, \dots, I_{in}$ のうちの1つを送ることになる。そして、商人との最初の取引について、 i 番目のユーザは、識別子 I_{i1} を商人に送ることになる。

【0018】その後、同じユーザと同じまたは異なる商人との間の次の取引について、そのユーザは、識別子 I_{i2} を送ることになる。識別子は各取引で変化するもので、長い期間について多数の取引に関する情報を有したとしても、商人は購入者についてのいかなる情報も見つけることは不可能である。そして、本発明は、上述したリンク可能性の問題を実質的に減少させる。

【0019】図1において、識別子 I_{ij} の受け取りにより、商人104は、その識別子を、その取引の間に、ユーザ102により注文された商品を含むパッケージ110のラベル108に付ける。この時点において、商人104は、ユーザ102のアイデンティティもユーザ102の住所も知らない。商人104は、この取引についてのユーザの識別子が I_{ij} であることを知り、配送業者106がパッケージ110をユーザ102に適切に配達できるように、ユーザ102が配送業者106と関係を有していることを知る。そして、商人104は、パッケージ110を配送業者106へ提供する。

【0020】パッケージ110の受け取りにより、配送業者106は、識別子 I_{ij} を決定するために、ラベル108を読み取る。ラベル108は、望ましくは、配送業者がラベルの読み取りを自動化できるように、機械読み取り可能なフォーマットになっていることに留意すべきである。勿論、ラベルの特定の機械読み取り可能なフォーマットは、識別子をラベル108に付ける際に商人104により使用される技法および識別子をラベルから読み取る際に配送業者106により使用される技法の両方を決定することになる。

【0021】一例として、商人は、バーコードスキャナを使用して配送業者により読み取り可能なバーコードラベルを印刷することができる。配送業者106が識別子 I_{ij} を読み取ると、配送業者106は、識別子とユーザの名前および住所との間の関連を記憶するデータベーステーブル114を含むデータベース112にアクセスする。図1に示されているように、テーブルは、各ユーザに対して複数の識別子を記憶する。例えば、ユーザ1に対して、テーブル114は、 n 個の識別子を記憶するように示されている。

【0022】配送業者106は、商人104から受け取ったパッケージ110について、ラベル108から読み取った識別子に関連づけられた名前および住所を決定するために、データベースルックアップを実行する。これらの識別子は、各識別子が1つのデータベース記録を独特に同定し、重複の可能性が極めて小さく、かつ存在しないと思われるということを保証するために十分に大きいように設計される。識別子の生成は、後述する。

【0023】受け取った識別子と一致する適切なデータベース記録を配送業者106が見つけると、配送業者106は、名前および住所のラベル116をパッケージ110に付け、パッケージ110はユーザ102に配送す

ることになる。そして、このようにして、ユーザ102は、商人104から商品を匿名に受け取る。委託された第三者である配送業者106のみが、識別子ユーザの名前および住所と関連させることができる。

【0024】上述したように、従来技術による匿名の配達方法にないこの技法の利点は、連続するオンライン取引の各々について異なる固有の識別子をユーザが使用するので、本発明による技法は、リンク可能でないことである。即ち、商人が取引情報を集めることができたとしても、そのような情報は、何れか一人の特定のユーザにリンクさせることは困難である。

【0025】ここに示されたステップは、配送業者により、プログラム可能なコンピュータを使用して、望ましくは実行され得ることに留意すべきである。そのようなコンピュータは、プロセッサによりアクセス可能なメモリ中に記憶されたコンピュータプログラムコードを実行するためのプロセッサを含む。ここで使用されているように、メモリの用語は、これに限定されるものでないが、ランダムアクセスメモリ(RAM)、リードオンリメモリ(ROM)、磁気ディスク、光ディスク、およびホログラフィックメモリを含む何れかのコンピュータで読み出し可能な媒体を指すために使用される。

【0026】望ましい実施形態において、コンピュータプログラムコードは、コンピュータプロセッサに接続されたRAMのような高速メモリに記憶される。本発明を実施するために必要とされるコンピュータプログラムコードは、何れかの周知のコンピュータ言語で書くことができる。本発明のこの説明により、当業者は、本発明を実施するために必要なプログラムコードを容易に書くことができる。

【0027】また、コンピュータは、周知の方法で、データベース112と通信することになる。ユーザは、周知の入出力装置および技法(例えば、ディスプレイスクリーン、キーボード、マウス)を使用してコンピュータと相互作用する。ここに説明されたタイプのプログラム可能なコンピュータは、この技術分野においてよく知られており、さらに説明する必要のないものである。

【0028】上述したスキームを正しく働かせるために、ユーザ102により使用される特定の識別子 I_i は、データベース114においてユーザの名前および住所と事前に関連づけられなければならない。この事前の関連づけを実行するために、様々な技法がある。

【0029】第1の実施形態において、特定のユーザにより使用されるべき識別子は、配送業者により前もって生成され、ユーザのコンピュータに記憶するためにユーザに提供される。例えば、ユーザ102が、ここで説明される匿名の配達サービスに加入することを望む場合、ユーザは配送業者106に登録し、一連の識別子を要求する。配送業者106は、 n 個のそのような識別子を生成し、これらの n 個の識別子をユーザに提供する。

【0030】配送業者は、これらの n 個の識別子をそのデータベーステーブル114に記憶する。そして、 i 番目のユーザに対して生成される n 個の識別子は、 $I_i^1, I_i^2, I_i^3, \dots, I_i^n$ となる。これらの同じ n 個の識別子 $I_i^1, I_i^2, I_i^3, \dots, I_i^n$ は、ユーザ i のコンピュータにも記憶されることになる。この実施形態によれば、配送業者が商人から識別子 I_i を受け取るとき、配送業者は、配送のための名前および住所を決定するために、その識別子を含む固有の記録を探す。

【0031】ある識別子が使用された後、それは、ユーザのコンピュータおよび配送業者のデータベース112の両方の記憶から削除され得る。これは、上述したように、各固有の識別子が、一度だけ使用されるからである。この実施形態は、ユーザのコンピュータおよび配送業者のデータベースの両方において多量の記憶を必要とすることが認識される。これは、特に、固有の識別子 I_i が、重複がないことを保証するためにかなり多数でなければならないという事実による。

【0032】本発明の別の実施形態によれば、ユーザおよび配送業者は、必要な場合に、ダイナミックに識別子を生成する。この実施形態において、ユーザが、サービスに対する加入者として配送業者に登録するとき、配送業者は、ユーザに対して固有のキーを提供する。 i 番目のユーザに対して、我々は、このキーを K_i と呼ぶ。配送業者は、ユーザに、カウンターについての初期値を提供する。 i 番目のユーザに対して、我々は、このカウンターを C_i と呼ぶ。

【0033】カウンターは、ユーザおよび配送業者の両方に知られた何らかの既知のインクリメントアルゴリズムに従って、増加的に変化することになる。例えば、このアルゴリズムは、 C_i から $C_i + s$ への単なる値の変化であり得る。ここで、 s は正または負の整数である。勿論、インクリメントアルゴリズムは、配送業者およびユーザの両方に知られたいかなるアルゴリズムであってもよい。

【0034】単純な表記として我々は、そのインクリメントアルゴリズムに従って一度インクリメントされたカウンター C_i を指すために、表記 $C_i + 1$ を使用する。この実施形態によれば、識別子 I_i は、ユーザおよび配送業者が、 K_i および C_i の知識を使用して I_i をダイナミックに生成できるように、 K_i および C_i の一方向関数(one-way function)として演算される。この関数は、 K_i および C_i が I_i の知識から決定され得ないという点で、一方向である。

【0035】この実施形態は、図2との関連で説明される。この実施形態において、ユーザ202が、商人204との取引に関わるとき、ユーザ202は、ユーザのコンピュータに記憶された K_i および C_i の値に基づいて、 I_i をダイナミックに生成し、この識別子 I_i を商人204へ送る。ユーザは、次の取引において、ユーザが異

なる I_{ij} を生成することになるように、インクリメントアルゴリズムに基づいて、 C_i の値を $C_i + 1$ へインクリメントする。配送業者の側で、配送業者206が、商人204から、ラベル208上に識別子 I_{ij} を含むパッケージ210を受け取るとき、配送業者206は、上述したように、一致する識別子を含む記録について、そのデータベース212をサーチする。

【0036】この実施形態によれば、配送業者のデータベース212は、図2に示されたデータベーステーブル214を記憶する。各ユーザ i について、データベーステーブル214は、カウンター C_i の現在の値を使用して生成された固有の識別子 I_{ij} 、ユーザの名前および住所、カウンター C_i の現在の値、インクリメントアルゴリズム、およびユーザのキー K_i を記憶する記録を含む。

【0037】配送業者206がラベル208上で受け取られた識別子 I_{ij} をデータベーステーブル214中に見つけるとき、配送業者は、その識別子に関連づけられた名前および住所を有するラベル216を印刷し、そのパッケージ210をユーザに配送する。この実施形態において、配送業者は、ユーザについてのデータベース記録を、以下のように更新する。配送業者は、インクリメントアルゴリズムに従って、記録中の C_i の値をインクリメントする。

【0038】そして、配送業者は、 K_i および更新された C_i の値に基づいて新しい識別子 I_{ij} を演算する。そして、この実施形態において、上述した実施形態の記憶の問題は、解決される。これは、ユーザおよび配送業者が、多数の事前に演算された識別子を記憶するのではなく、固有の識別子をダイナミックに生成するために必要とされる情報をユーザおよび配送業者が記憶するからである。

【0039】識別子がダイナミックに生成される上述した実施形態の1つの可能性のある問題は、ユーザおよび配送業者が、適切な同期を保たなければならないことである。即ち、ユーザおよび配送業者により保持されるカウンター C_i の値は、同じでなければならない。さもなければ、ダイナミックに生成される識別子は、一致しないことになる。同期化の問題を解決するためのいくつかの方法がある。まず、ユーザが識別子 I_{ij} を商人に送る状況を考える。

【0040】そして、ユーザは、上述した技法に従って、そのカウンター C_i をインクリメントする。しかし、商人がそのラベル上に識別子 I_{ij} を有するパッケージを送ることに先立って、商人のコンピュータが、クラッシュし、そして商人が、取引に関する情報を失い、配送業者が、商人から識別子 I_{ij} を受信しない。そして、配送業者は、この特定のユーザに関連づけられたカウンター C_i をインクリメントすることがなく、ユーザのカウンター C_i および関連づけられた配送業者のカウンタ

ー C_i が、同期外れになっている。

【0041】このユーザの次の取引において、ユーザは、インクリメントされたカウンター（即ち、 $C_i + 1$ のカウンター値）に基づいて次の識別子を生成することになるが、その識別子の受け取りにより、配送業者は、そのデータベース中にその識別子を言い出すことができなくなる。これは、そのユーザに対する記録が、 C_i のインクリメントされていないカウンター値を使用して生成された識別子を含むからである。

【0042】ユーザおよび配送業者を同期外れにする別のやり方は、以下の通りである。ユーザが第1の商人との取引に入り、識別子 I_{ij} をその商人に送ることを考える。そして、ユーザは、上述した技法に従ってそのカウンター C_i をインクリメントする。ユーザは、第2の商人との別の取引に入り、インクリメントされたカウンター値 $C_i + 1$ に基づいて、次の識別子 I_{ij+1} を第2の商人に送る。しかし、第2の商人のパッケージは、配送業者に最初に到着し、配送業者は、識別子 I_{ij} を受け取る前に識別子 I_{ij+1} を受け取る。この時点において、このユーザに対する配送業者のデータベース記録は、識別子 I_{ij} を含んだままである。したがって、このシステムは、同期外れとなり、適切に動作しないことになる。

【0043】同期外れ問題の1つの解決法は、図3に示されたようなデータベース302を構成しかつ保持することである。この実施形態において、一連の識別子が、各ユーザに対して記憶される。テーブル302は、 i 番目のユーザに対する記憶された記録を示す。テーブル302は、識別子 I_{i1} , I_{i2} , I_{i3} , ..., I_{in} を含む n 個の記録を記憶する。これらの識別子は、 i 番目のユーザのキー K_i および i 番目のユーザのカウンター C_i の $C_i + (n - 1)$ への増分値を使用して生成される。

【0044】そして、配送業者が、（カウンター値に基づいて）期待された特定の順序で識別子を受け取らない場合であっても、配送業者は、テーブル302中のマッチング記録を受信された識別子に恐らく一致させることになる。 n の値は、配送業者のデータベースの記憶容量と配送業者が取り扱うことを望む非同期の程度のバランスとして選択され得る。

【0045】別の技法によれば、ユーザおよび配送業者が値 n より大きい量だけ同期外れになったとしても、配送業者は、それにも関わらず、以下のように識別子を取り扱うことができる。図3に示された実施形態において、配送業者が、データベーステーブル302中に存在しない識別子を含むパッケージを受け取ったと考える。配送業者は、その時点において、識別子が無効であり、パッケージの処理を終了させることを仮定することができる。

【0046】しかし、配送業者は、以下のように、パッケージに関連づけられたユーザを決定することを試みるために、データベーステーブル302中の存在するデー

タを外挿することを試みることができる。配送業者は、データベーステーブル302において、ユーザの各々に対する連続する x 個の識別子を計算することを試みることになる。例えば、 $x=3$ である場合、図3に示された i 番目のユーザに関して、配送業者は、そのユーザに対して最後に記憶された識別子の直後に続くシーケンス中の3個の識別子を計算することになる。

【0047】したがって、図3に示された実施形態において、配送業者は、各ユーザに対して n 個の記録を記憶し、 i 番目のユーザに対する最後の記録は、 I_{i^n} であり、配送業者は、それぞれ C_{i+n} , C_{i+n+1} , C_{i+n+2} の増分カウンター値を使用して $I_{i^{n+1}}$, $I_{i^{n+2}}$, $I_{i^{n+3}}$ をダイナミックに計算することになる。この外挿は、図3において306として示されているように、配送業者が別の x 個のデータベーステーブル記録を生成することと考えられ得る。配送業者は、新たに生成された識別子のうちの1つが受信された識別子と一致するまで、または配送業者が、受け取った識別子がユーザに一致しないと決定するまで、ユーザの各々に対するこの x 個の記録の外挿を実行することになる。

【0048】上述した実施形態において、複数の記録が、各ユーザに対して記憶され、あるタイプのテーブルメンテナンスが、合理的なサイズ内にデータベーステーブルを保持するために実行されなければならない。例えば、配送業者が各ユーザに対して10個の記録を記憶すると考えると、 i 番目のユーザに対して、データベーステーブルは、以下の識別子を含む記録を有する。即ち、 I_{i^1} , I_{i^2} , I_{i^3} , ..., $I_{i^{10}}$ である。配送業者が、商人からのパケットラベル上に識別子 I_{i^8} を受け取ったと考える。配送業者は、その識別子を、 i 番目のユーザに一致させ、パッケージを上記したように、そのユーザに配送する。

【0049】配送業者は、何らかの同期エラーが生じ、配送業者は、そのユーザとの関連で何らかのより速いシーケンス識別子を受け取ることには恐らくならないという仮定をなすことができる。そして、テーブルメンテナンス動作に従って、配送業者は、識別子 I_{i^1} , I_{i^2} , I_{i^3} , ..., I_{i^6} を含む記録を削除することができる。これは、これらの識別子は、このユーザに関連して恐らく受信されないからである。識別子 I_{i^7} を含む記録は、データベース中に残っており、更なる同期の問題のために、ユーザはその識別子を依然として使用することができる。

【0050】更なる別の実施形態において、ユーザは、識別子 I_{i^1} およびその識別子を生成するために使用されたカウンター C_i の両方を商人に供給することができる。この実施形態は、配送業者が、以下のように、新しい識別子をより容易に外挿することを可能にする。配送業者が、この特定のユーザに対して記憶され、以下の識別子、即ち I_{i^1} , I_{i^2} , I_{i^3} , ..., $I_{i^{10}}$ を含む10個の

記録を有すると仮定する。そして、ユーザおよび配送業者が、同期外れとなっており、ユーザが識別子 $I_{i^{14}}$ を商人に送るようになっていないと仮定する。

【0051】また、この実施形態によれば、ユーザは、商人に C_{i+13} も送る。これは、識別子 $I_{i^{14}}$ を演算するために使用されたカウンター値である。図3において、識別子 I_{i^n} が、カウンター値 $C_{i+(n-1)}$ を使用して生成されたことを思い出されたい。そして、商人は、パッケージ上に、 $I_{i^{14}}$ および C_{i+13} を含むラベルを付ける。このパッケージの受領により、配送業者が、データベーススルックアップを実行するが、識別子 $I_{i^{14}}$ を発見しない。

【0052】上述した外挿技法に従って、配送業者は、ユーザの各々に対する新しい識別子を生成することを試みることができる。しかし、上述したように、外挿の数 $x=3$ である場合、このユーザに対して、配送業者は、 $I_{i^{11}}$, $I_{i^{12}}$, $I_{i^{13}}$ をダイナミックに生成し、受け取られた識別子 $I_{i^{14}}$ は、一致しないことになり、パッケージは配達されないことになる。

【0053】しかし、この実施形態によれば、配送業者は、初期のデータベーススルックアップを実行するが、識別子 $I_{i^{14}}$ を発見しない場合、配送業者は、この場合 C_{i+13} であるラベル上のカウンター値を参照することになる。配送業者は、受け取られたカウンター値 C_{i+13} と共にユーザのキーを使用するシステムにおいて、ユーザの各々に対する識別子を生成することを試みることになる。そして、配送業者は、適切な識別子を生成し、データベース一致となるチャンスを改善しつつ、ユーザあたりの外挿を一度のみ必要とする。

【0054】この技法の更なる改良において、配送業者は、速いデータベース一致の可能性を向上させるために、ユーザに対して特定の順序で識別子を外挿しかつ生成することができる。例えば、配送業者は、特定のユーザに対して最高のカウンター値が現在記憶されていることを知っているので、配送業者は、特定のユーザに対してデータベース中に記憶されたカウンター値の範囲が、商人から受け取ったカウンター値を既に超えている場合、この特定のユーザは問題となる識別子を生成したことは恐らくなく、配送業者は、このユーザをスキップし、識別子をダイナミックに生成しないと決定することができる。

【0055】さらに別の性能改善によれば、配送業者は、最も可能性のあるユーザに対する識別子が最初に試みられるように外挿を命令するように試みることができる。例えば、特定のユーザが C_i ないし C_{i+10} の範囲中のカウンター値を含む記憶された記録を有し、配送業者がカウンター C_{i+11} をラベル上で受け取った場合、配送業者は、カウンターが1つのインクリメントにより同期外れとなっただけであるので、このユーザはたぶん外挿の候補であると判断することができる。

【0056】上述した識別子と共にカウンター C_i をユーザが送る技法は、限定された数の場合において、商人が、所定の購入を特定のユーザと関連づけることを可能にすることに留意すべきである。例えば、商人がカウンターを受け取るので、商人は、これらのカウンターを集め、インクリメントアルゴリズムの何らかの決定を行い、何らかの取引間の相関をなすことができる。例えば、長い時間について、商人が、以下の識別子とカウンターとの組合せを受信したと仮定する。

【0057】

| TX ID | 識別子 | カウンター |
|-------|--------------|-------|
| 1 | 123324384895 | 1 |
| 2 | 139483948395 | 129 |
| 3 | 957395739584 | 2 |
| 4 | 494958928923 | 55 |
| 5 | 957802852949 | 131 |
| 6 | 958395038503 | 88 |
| 7 | 472395023782 | 133 |
| 8 | 594848582385 | 3 |

【0058】カウンターの分析により、商人は、取引識別子(TX ID) 1, 3および8に同じユーザが関連づけられているという仮定を非常によく行うことができる。これは、 $C_i = C_i + 1$ のインクリメントアルゴリズムに関連づけられる取引のためのカウンターが、それぞれ1, 2および3であるからである。同様に、商人は、同じユーザがTX ID 2, 5および7に関連づけられているという過程を行うこともできる。これは、 $C_i = C_i + 2$ のインクリメントアルゴリズムに関連づけられた取引のためのカウンターが、それぞれ129, 131および133であるからである。勿論、これらの例は、商人により行われ得る分析の単純な例であるが、商人にカウンター値を提供することの可能性のある危険を示している。

【0059】上述した相関を防止するために、本発明の別の実施形態によれば、ユーザは、識別子 I_i およびその識別子を生成するために使用されたカウンター C_i の暗号の両方を商人に供給する。望ましくは、配送業者は、周知の公開鍵/秘密鍵暗号化スキームに従って公開鍵/秘密鍵の対の公開鍵部分をユーザに提供する。ユーザは、公開鍵を使用してカウンター C_i を暗号化する。配送業者の公開鍵は、 PK_s で表され、公開鍵 PK_s を使用するカウンター C_i の暗号は、 $E_{PK_s}(C_i)$ で表される。

【0060】ユーザは、 I_i および $E_{PK_s}(C_i)$ を商人に送る。そして、商人は、これらのパラメータを配送業者に送る。上述したものと同様に、配送業者は、そのデータベース中に一致する識別子 I_i を有する記録を見つけない場合、カウンターを解読し、それを上述した新しい識別子を外挿するために使用することができる。しかし、この場合において、商人により受け取

られたカウンターは暗号化されており、したがって、商人は、カウンターからいかなる有用な情報も発見することができない。

【0061】 $E_{PK_s}(C_i)$ は、かなり大きく、商人が、標準的配送ラベル上の暗号化されたカウンターを復号化することは困難であることに留意すべきである。そして、この実施形態の変形において、商人は、識別子 I_i のみを配送ラベル上に付けることができる。配送業者が、そのデータベース中に一致する識別子を有する記録を発見できない場合にのみ、配送業者は、商人から関連づけられた $E_{PK_s}(C_i)$ を要求する。商人は、 I_i および $E_{PK_s}(C_i)$ を含む別のラベルを送ることができるか、または $E_{PK_s}(C_i)$ は、商人から配送業者に電子的に送信され得る。

【0062】我々は、ユーザおよび配送業者が、カウンターを使用することなしに、必要な場合に、識別子をダイナミックに生成する本発明の別の実施形態を説明する。図2との関連で上述したものと同様に、 i 番目のユーザが、そのサービスに対する加入者として配送業者に登録している場合、配送業者は、ユーザに、固有のキー K_i を提供する。この固有のキー K_i は、ユーザおよび配送業者の両方に知られている。この実施形態における識別子 I_i は、 K_i の一方関数および各取引についてユーザにより生成されるランダム数 R として演算される。

【0063】この実施形態は、図4との関連で説明される。ユーザ402が、商人404との取引に関わっているとき、ユーザ402は、 K_i の値およびユーザ402により生成されるランダム数 R に基づいて、 I_i をダイナミックに生成する。ユーザ402は、識別子 I_i およびランダム数 R を商人404へ送る。商人404は、パッケージ410のラベル408上へ、識別子 I_i およびランダム数 R を付け、そのパッケージを配送業者406へ提供する。

【0064】この実施形態によれば、配送業者のデータベース412は、図4に示されたようなデータベーステーブル414を記憶する。各ユーザ i に対して、データベーステーブル414は、ユーザの名前および住所およびユーザのキー K_i を記憶する記録を含む。配送業者406はパッケージ410を受け取るとき、配送業者406は、ラベル408上の識別子 I_i およびランダム数 R を読み取る。そして、配送業者は、ユーザ402が受け取られた識別子を生成するために使用した同じ一方関数と共に、受け取られたランダム数 R を使用して、データベーステーブル414中のキー K_i の各々を使用して新しい識別子を生成する。

【0065】配送業者は、生成された識別子のうちの1つが受け取られた識別子と一致するまで識別子を生成し続ける。一致する識別子が生成されたとき、配送業者は、その一致する識別子を生成するために使用されたキー K_i が、そのパッケージに関連づけられた i 番目のユ

ーザに属することを知り、配送業者は、テーブル 414 から i 番目のユーザの関連する名前および住所を読み出すことができる。配送業者は、ユーザの名前および住所を有するラベルを印刷し、パッケージをユーザに配送する。

【0066】この実施形態は、いくつかの場合において、カウンターを使用する上述した実施形態はより演算的に集約的であるが、この実施形態は、配送業者またはユーザがいかなる状態情報（例えば、カウンター値）を保存する必要がないので、カウンターの実施形態の同期の問題を解決する。また、この実施形態は、配送業者が、受信したランダム数を使用してユーザについてのいかなる情報も決定することを許容しない。

【0067】ランダム数が、識別子のダイナミックな生成に使用される別の実施形態は、以下の通りである。この実施形態において、ユーザは、ランダム数 R に付加された彼／彼女の住所を暗号化することにより識別子を生成し、暗号化されたテキストを商人に送る。商人は、暗号化されたテキストをラベルに付け、パッケージを配送業者に提供する。パッケージの受け取りにより、配送業者は、暗号化されたテキストを読み取り、暗号化されたテキストを解読し、ユーザの名前および住所を抽出する。この実施形態において、配送業者は、暗号化されたテキストを解読するために使用され得るキーのみを記憶する必要がある。公開鍵／秘密鍵暗号化スキームを含む様々な周知の暗号化技法が、この実施形態に関連して使用され得る。

【0068】図 5 を参照して、商人に対する金銭の支払いの認証について説明する。上述したように、匿名のエレクトロニックコマースについての問題の 1 つは、支払いがユーザから商人になされなければならないということである。そのような支払いは、一般に、クレジットカードによりなされるので、商人が、支払いを処理するためにユーザの名前を知らなければならない。これは、匿名のエレクトロニックコマースの可能性を厳しく制限する。

【0069】支払いが、別の委託された第三者を通してなされ得るが、そのような委託された第三者の支払いを受けるもの、委託された第三者の配送業者、購入者および商人の組合せを調整することはロジスティック的に困難である。そして、本発明の以下に説明する別の実施形態において、我々は、上述した匿名の配達技法との組合せで使用され得る改良された支払い技法を提供する。この実施形態によれば、商人は、配送業者から支払いを受け取り、配送業者は、ユーザからその支払額（任意の取引処理料をプラスして）取り戻すことができる。

【0070】この実施形態において、識別子 I_{ij} は、上述したように、ユーザによりダイナミックに生成されるが、識別子は、2 つの部分 $part1(I_{ij})$ および $part2(I_{ij})$ に分けられる。例えば、 I_{ij} が 32 ビットであ

る場合、第 1 の 16 ビットは、 $part1(I_{ij})$ となり、第 2 の 16 ビットは、 $part2(I_{ij})$ となる。図 5 に示されているように、配送業者のデータベーステーブル 514 は、識別子のこれらの 2 つの部分記憶する。ユーザ 502 は、電子的取引に関連づけられた支払い認証のために使用される $message$ を生成する。

【0071】例えば、典型的な $message$ は、「100 ドルを支払え」であり得る。そして、ユーザ 502 は、識別子の第 2 の部分を周知のメッセージ認証コード (MAC) キーとして使用する一方で、MAC 技法に従ってメッセージを暗号化することによりシークレット S_i を、

$$S_i = MAC_{part2(I_{ij})}(message)$$

として生成する。商人 504 との取引の完了により、ユーザ 502 は、 $part1(I_{ij})$ 、 S_i 、 $message$ 、 $E_{PK_i}(C_i)$ のパラメータを商人 504 に送る。これらのパラメータの受け取りにより、商人 504 は、ユーザ 502 により注文されたアイテムを含むパッケージ 510 に対するラベル 508 を用意し、パッケージ 510 を配送業者 506 へ送る。

【0072】上述したように、ユーザ 502 により商人 504 に送られるパラメータは、パッケージラベル 508 上に好都合に符号化されるには長すぎる可能性があり、パラメータのいくつかは、破線 530 により図 5 中に示されたように別の方法で（例えば、電子的に）、商人 504 により配送業者 506 へ送信され得る。望ましくは、ラベル 508 は、識別子 $part1(I_{ij})$ を含み、その識別子に関連づけられた他のパラメータ、即ち S_i 、 $message$ 、 $E_{PK_i}(C_i)$ は、配送業者に電子的に送信される。

【0073】パッケージ 510 の受け取りにより、配送業者 506 は、ラベル 508 上にある $part1(I_{ij})$ についてデータベースサーチを行う。発見されると、配送業者 506 は、データベース記録から関連する $part2(I_{ij})$ および商人 504 から電子的に受信された $message$ を取り、シークレット

【数 2】

$$S_i = MAC_{part2(I_{ij})}(message)$$

を演算する。演算されたシークレット S_i が商人 504 から電子的に受信されたシークレット S_i と一致する場合、配送業者 506 は、ユーザ 502 が $message$ 中で特定された価格を支払うことに同意したに違いないと決定する。これは、そうでない場合、商人 504 は、配送業者 506 により演算されたシークレット S_i に一致するシークレット S_i を演算することはできなかったからである。

【0074】この場合において、配送業者506は、商人504に、メッセージ中に特定された額を支払い、パッケージ510をユーザに配達し、ユーザ502に、配送料、配送業者が商人に支払った額、プラス支払いを取り扱うための適切な取引量を課金することができる。演算されたシークレット S_i が商人504から受け取ったシークレット S_i と一致する場合、ユーザ502は、支払いをすることに同意したことを否定できない。

【0075】演算されたシークレット S_i が、商人504から受け取ったシークレット S_i と一致しない場合、問題があり、適切な例外処理が行われる。パッケージ510の受け取りにより、配送業者506がデータベース512中にpart1(I_i)を見つけることができない場合、上述した外挿技法が使用され得る。

【0076】以上の詳細な説明は、例示的なものと理解されるべきであり、限定的ではなく、ここに開示された発明の範囲は、詳細な説明により決定されるべきでなく、特許法により許容される範囲に従って解釈される特許請求の範囲から解釈されなければならない。ここに示された実施形態は、本発明の原理を単に例示したものであり、様々な修正が、当業者により本発明の範囲および精神から離れることなしになされ得る。例えば、送られるパラメータ、およびそのようなパラメータの暗号化に対する様々な修正および変形が、当業者にとって容易に明らかとなるであろう。例えば、ユーザは、ユーザの識別子を表す i の暗号化された値および/または配送業者に渡された場合、データベーススルックアップの性能を改良し得る他の暗号化されたパラメータを商人に渡すことができる。

【0077】

【発明の効果】以上説明したように、本発明によれば、エレクトロニックコマースにおけるリンク可能でない匿名性配達技法を提供することができる。

【0078】特許請求の範囲の発明の要件の後に括弧で記載した番号がある場合は本発明の一実施例の態様関係を示すものであって、本発明の範囲を限定するものと解釈してはならない。

【図面の簡単な説明】

10 【図1】本発明の一実施形態を示すために使用されるエレメントの構成を示す図。

【図2】本発明の別の実施形態を示すために使用されるエレメントの構成を示す図。

【図3】本発明の実施形態によるデータベース記録の内容およびデータベース情報の外挿を示す図。

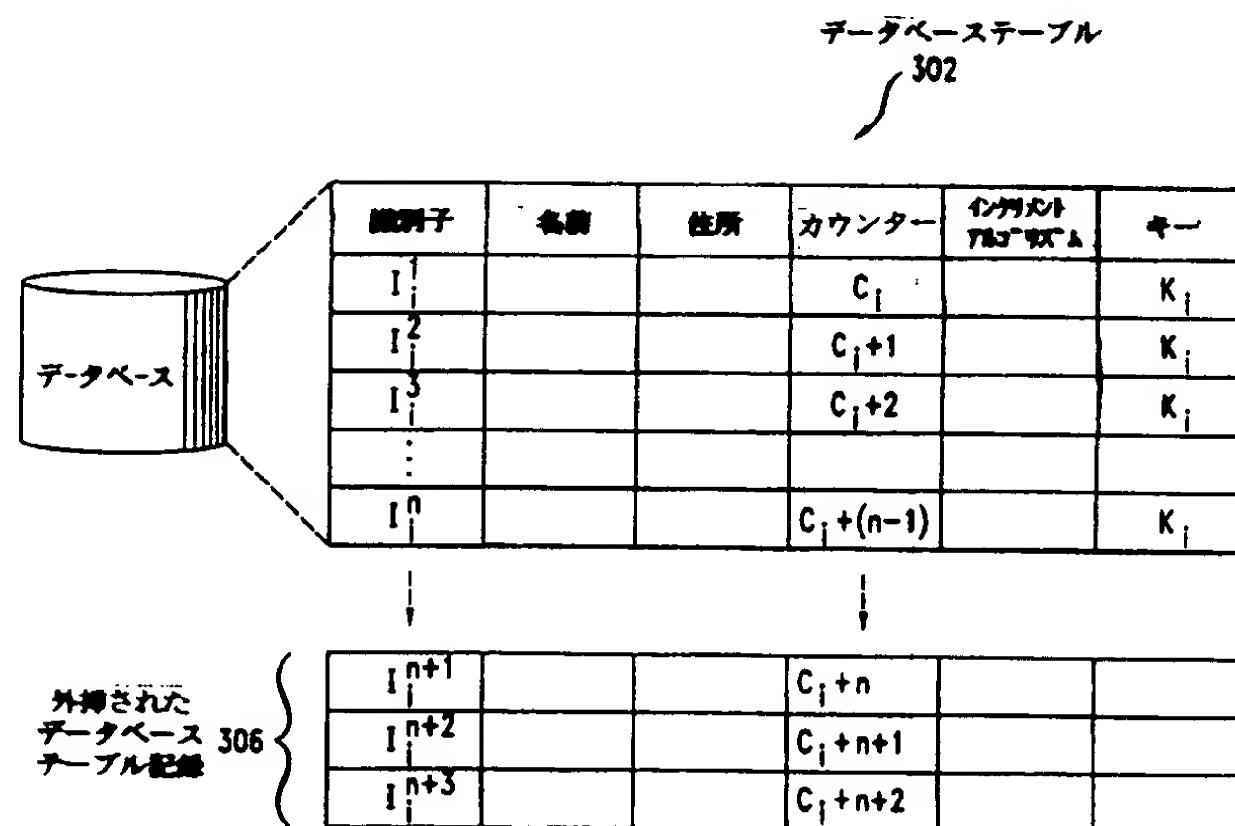
【図4】本発明の別の実施形態を示すために使用されるエレメントの構成を示す図。

20 【図5】支払い技法が配達技法に結合される本発明の一実施形態を示すために使用されるエレメントの構成を示す図。

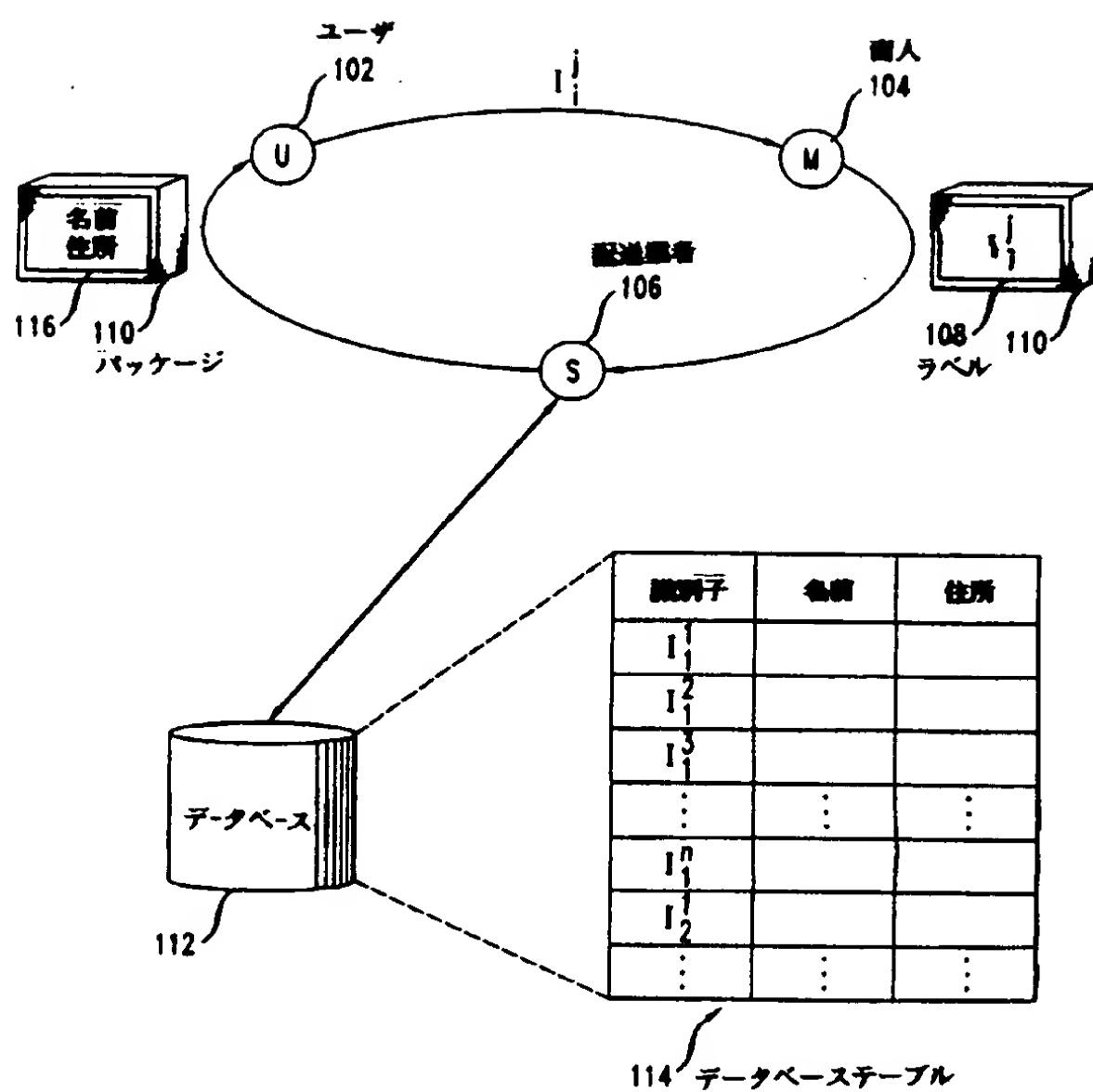
【符号の説明】

102, 202, 402, 502 ユーザ
104, 204, 404, 504 商人
106, 206, 406, 506 配送業者
108, 208, 408, 508 ラベル
110, 210, 410, 510 パッケージ
112, 212, 412, 512 データベース
114, 214, 414, 514 データベーステーブル

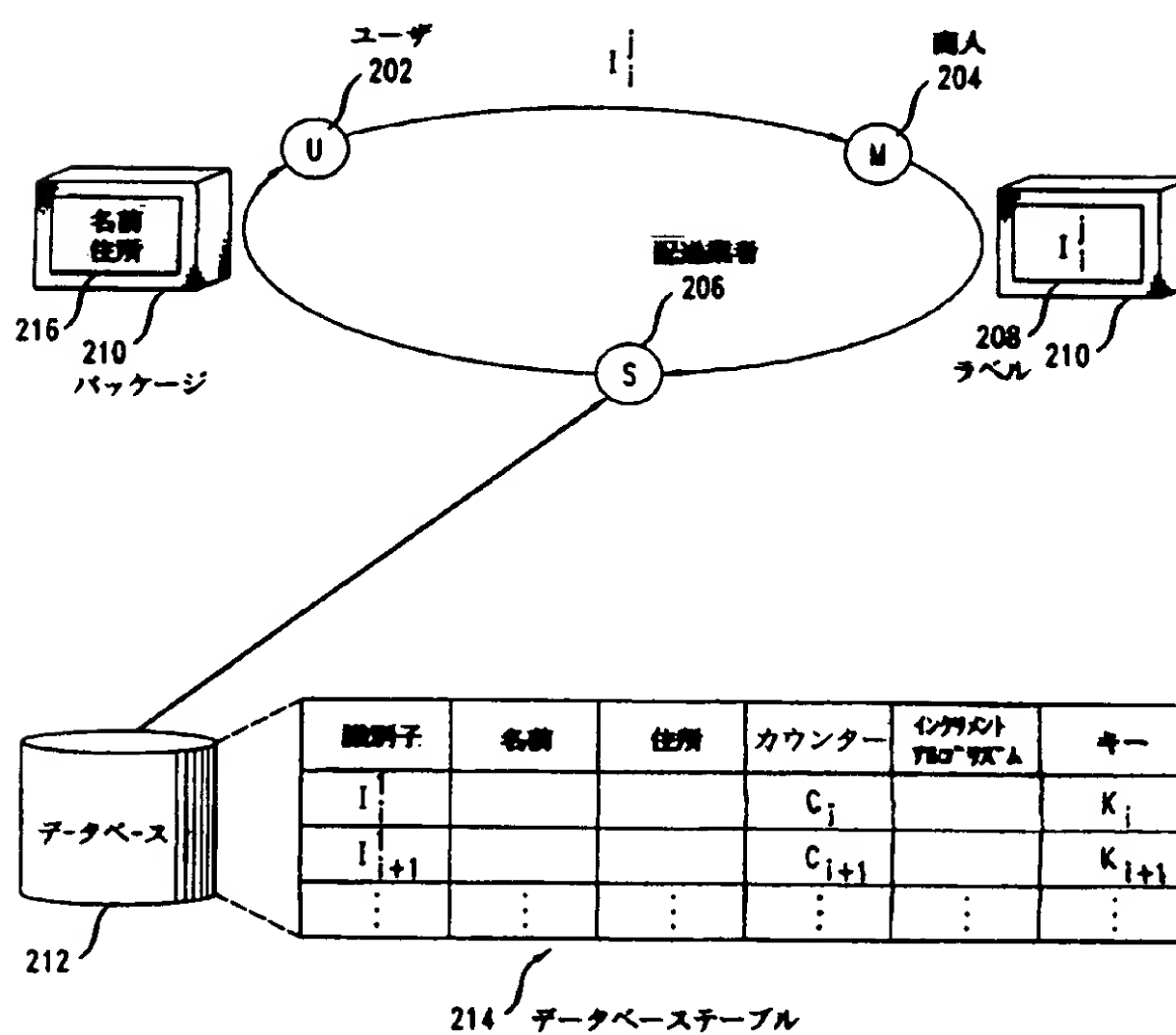
【図3】



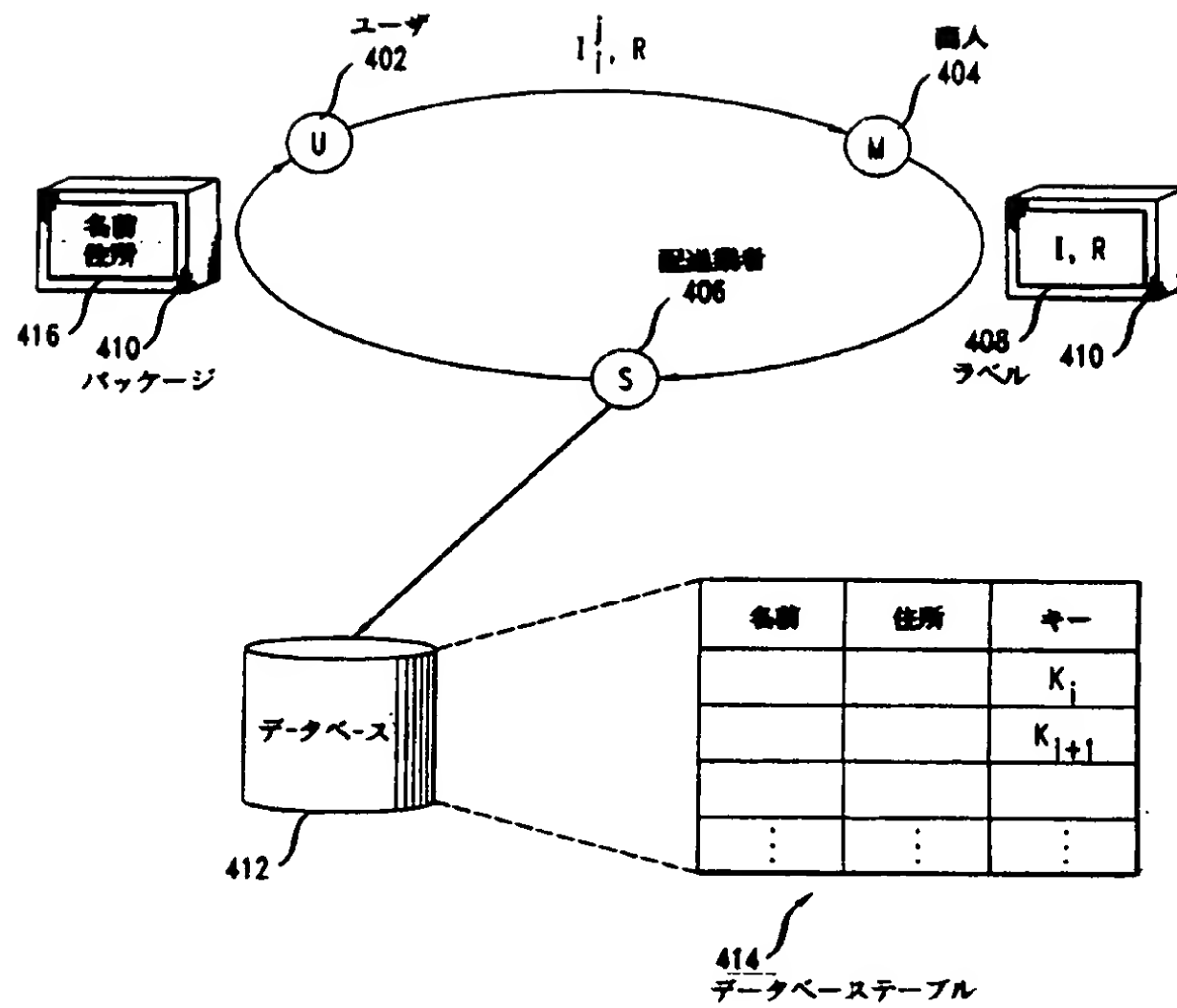
【図 1】



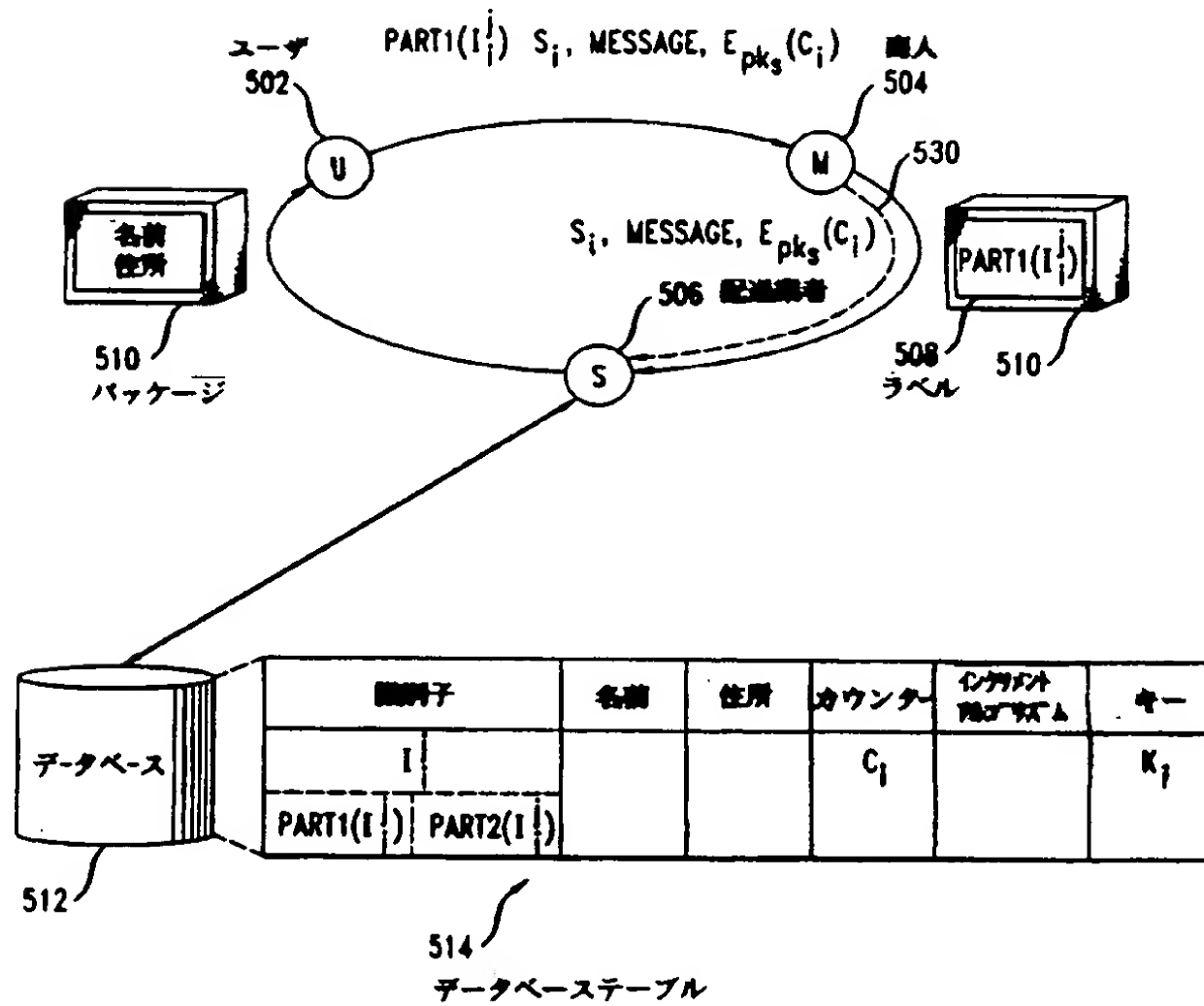
【図 2】



【図4】



【図5】



フロントページの続き

(71)出願人 596077259

600 Mountain Avenue,
Murray Hill, New Jersey 07974-0636 U. S. A.

(72)発明者 ビョーン エム ジャコブソン
アメリカ合衆国、07030 ニュージャージー
州、ハウボウカン、ガーデン ストリー
ト 1203

(72)発明者 マイケル ケンドリック ライター
アメリカ合衆国、08869 ニュージャージー
州、ラリタン、ブルーバード ウェイ
4

(72)発明者 アブラハム シルバーシャッツ
アメリカ合衆国、07059 ニュージャージー
州、ウォラン、ウルフ ヒル ドライブ
48